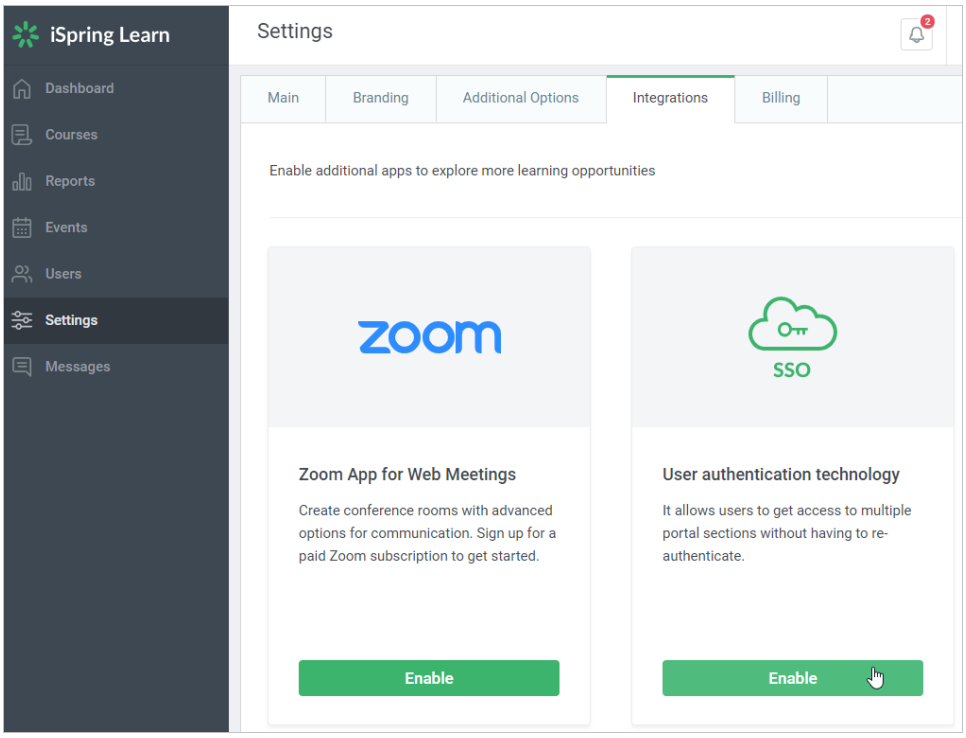
SAML Authorization

iSpring Learn allows you to use SAML to enable single sign-on to the account.

Important: authorization with SAML doesn't work in the mobile application.

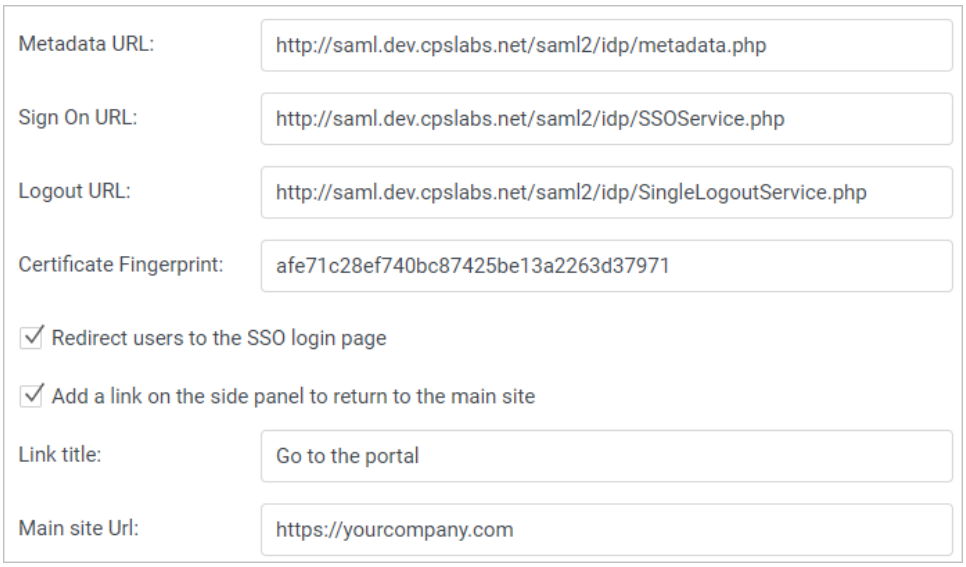
To set up SAML authentication in your account:

1. Go to the **Settings** section, then open the **Integrations** tab and, in the **SSO** area, hit **Enable**.

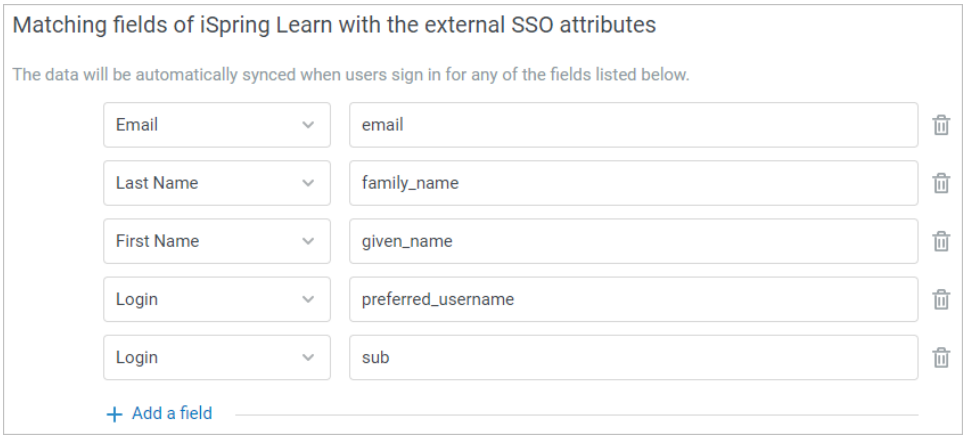


2. Fill out the form fields, adding URL and other details of your identity provider. The latter is the resource your users are supposed to use for the initial authorization on your corporate portal.

Metadata Url	Link to your identity provider server pointing to the metadata file.
Sign On Url	Path to the server script which generates SAML identifier confirmation requests to handle authorization.
Logout Url	Path to the server script which generates SAML identifier confirmation requests to handle logout.
Certificate Fingerprint	Short version of the public key certificate for verifying a digital signature. It is used to confirm signing requests issued by an identity provider. Learn more about certificate fingerprints here.
Redirect users to the SSO login page	If this option is enabled, the iSpring login page will have the following URL: https://yourcompany.ispringlearn.com/sso/login.
Add a link on the side panel to return to the main site	A link to a resource specified by the administrator will appear on the sidebar.



3. If needed, match fields in iSpring Learn and your SSO service.



4. Click **Enable.**

Setting Up SAML on the Server

We recommend that you should use the SimpleSamlPhp library to set up your identity provider server to enable authorization with SAML 2.0.

Setting Up iSpring Learn

Configuration of your iSpring Learn account is completed by our employees. Just provide us with the following information:

1. Identity provider URL
2. SSL certificate (server.crt)
3. Secret key (server.pem)
4. certFingerprint for a quick verification

Setting Up Identity Provider

To set up the identity provider, perform the following steps:

1. Enable support of SAML 2.0 and Shibboleth 1.3 in the **config/config.php** file.

```
'enable.saml20-idp' => true, 'enable.shib13-idp' => true,
```

2. Switch on the authorization module. Different authorization modules are located in the **modules** folder. Open the folder where the needed method is located and create an empty file called enabled in it.

3. Enable the authorization module in the config/authsources.php file.
Important: email is a required attribute.

```
$config = array( 'example-userpass' => array( 'exampleauth:UserPass', 'student:studentpass' => array( 'uid' => array('student'), 'email' => 'student@example.com', 'eduPersonAffiliation' => array('member', 'student'), ), 'employee:employeepass' => array( 'uid' => array ('employee'), 'email' => 'employee@example.com', 'eduPersonAffiliation' => array('member', 'employee'), ), ), );
```

4.Configure the identity provider in the **saml20-idp-hosted** configuration file as in the example below.

```
'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri', 'authproc' => array( // Convert LDAP names to oids. 100 => array('class' => 'core:AttributeMap', 'name2oid'), ),
```

5. Add information about the identity provider into the **metadata/saml20-sp-remote.php** file.

```
$metadata['https://sp.example.org/simplesaml/module.php/saml/sp/metadata.php/default-sp'] = array( 'AssertionConsumerService' => 'https://sp.example.org/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp', 'SingleLogoutService' => 'https://sp.example.org/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp', );
```

If you have enabled SAML in your iSpring Learn account and for some reasons can't login using single sign-on, type the following web address: https://yourcompany.ispringlearn.com/login?no_sso.

Now you will sign in with the account as usual, using your login and password.

Useful links on SAML authorization:

Configuring SAML 2.0 SSO with Microsoft Active Directory Federation Services

Setting Up SAML for G Suite

Configuring SAML with Azure AD